DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

JUN 18 2003

MEMORANDUM FOR KEN HOCKENBERRY
DIRECTOR, WORKLOAD MANAGEMENT BRANCH
M:I:EO:OR:WM

FROM: Mary Ronan
Acting Privacy Advocate CL:PA

SUBJECT: Enterprise File Transfer Utility System (EFTU)
Privacy Impact Assessment (PIA)

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment for the Enterprise File Transfer Utility System. Based on the information you provided, we do not have any privacy concerns that would preclude this system from operating. However, a revised PIA is required when considering any future upgrades or modifications to the system.

We will forward a copy of the PIA to the Modernization Information Technology & Security Services Mission Assurance, Certification Program Office M:S:A:C and the Security Policy Support and Oversight Office M:S:S to be included in the Security Accreditation Package for formal acceptance for operation. The Security Policy Support and Oversight Office, which has security oversight responsibility, may request information concerning the statements contained in the PIA to ascertain compliance with applicable requirements.

If you have any questions, please contact me at 202-927-5170 or Gino Talbot at 202-622-2302.

Attachment

cc: Director, Modernization Information Technology Security Services
Certification Program Office M:S:C:C
Director, Security Policy Support and Oversight Office M:S:S

PRIVACY IMPACT ASSESSMENT

COVER SHEET

Title of System: Enterprise File Transfer Utility (EFTU)

Is this a new system, or an existing system? Existing system with enhancements. EFTU will use the existing Hardware configuration of the Enterprise FTP Network Server (EFNS). EFTU will provide updated operational software, and clustered database software. EFTU agents will communicate with the EFTU control (production) servers using secure **Application Messaging and Data Access Services (AMDAS)** (MQ-Series) messaging. EFTU is a utility that provides controlled file transfers between internal IRS systems. EFTU employs high availability clusters of control servers at two computing centers (MCC, TCC). The EFTU system will have agents on all IRS platforms needing the service – Current Production Environment (CPE) and Modernized.

If an existing system is this submission because of: (circle)
Modification
Re-certification with no-change
Modernization project

If this PIA is for a modernization project, circle the milestone:
One
Two
Three
Four
Final implementation

List all Systems of Records Notices (SORNs) under which this system operates. (Provide documentation from Headquarters Disclosure Office)

David Silverman concurrs that this system does not require a SORN, the server is infrastructure and not a Privacy Act record.

Name, Title, Mailing Address of System Owner:

Ken Hockenberry
Director Workload Management Branch
5000 Ellin Road
Lanham, MD 20706

Privacy Impact Assessment – ENTERPRISE FILE TRANSFER UTILITY

System Owner's Operating/Functional Division: M:I:EO:OR:WM

PIA Preparer/email/phone: Paul J. Biro/Paul.J.Biro@irs.gov/202-283-3529

Subject matter contact/email/phone:

Paul J. Biro/Paul.J.Biro@irs.gov/202-283-3529

Introduction

The Enterprise File Transfer Utility (EFTU) uses the existing EFNS servers at the two Computing Centers in Martinsburg and Tennessee (MCC and TCC).

EFTU agents will communicate with the EFTU control servers using secure AMDAS (MQ-Series) messaging. AMDAS messages provide for authentication, authorization, status and control. EFTU agents initiate transfers via standard FTP services, set up by agents according to the transfer rules established when a file transfer is approved by management and security (Form 12038 plus rules definition). The Form 12038 is used to authorize File Transfer Protocol (FTP) data transfers.

Transfers can be initiated by application program calls using the EFTU Application Interface (API), or by script or command line invocation of the agent API. All file transfers must be pre-approved and have entries in the12038 authorization database on the EFTU Control Servers.

EFTU Agent Processing

The EFTU agent on each source or destination platform includes the following categories of code: (note that any platform can be both a source and a destination for different transfers):

- Agent Initialization Code
- API Transfer-Initiation Code –
- Source-System Agent Code
- Destination-System Agent Code
- Status Request API Code

Each platform also includes an FTP client and server.

Agent Initialization will be accomplished by establishing an AMDAS connection to EFTU Server system queues.

API Transfer-Initiation

API Transfer-Initiation will be done through the use of Multi-threaded API Code to receive file transfer requests via application calls or scripted execution. This will verify parameters (Calling Sequence varies by type of transfer but will always include a File Transfer Identifiers which must match a pre-approved 12038 database entry). Will communicate requests to EFTU Server system, get return verification of authorization or error, and provide local error handling.

Source-System Agent -

Source-System Agent will issue a multi-threaded code to receive file-transfer initiation requests via encrypted AMDAS from the EFTU Control Server, including credentials for FTP service on this platform. It will also calculate Hash on file(s) to be transferred and communicate value to EFTU Control Server.

If the initiation request indicates that the transfer requires a matching disclosure audit data file, calculate the disclosure file hash and send to EFTU Control Server, and FTP transfer (upload) the disclosure audit data file to the EFTU Control Server disclosure file directory, and get a successful status. Disclosure files are handled (transparently) just like other files, but the delivery rules specify that the second

(data) file cannot be sent until the first (disclosure) file has been successfully transferred via "chained point-to-point" to its final destination (SAAS).

EFTU will be dynamically configured with directory/filename of authorized file as available to authorized destination system only. For local error handling, the system will communicate status back to the EFTU Control Server.

Destination-System Agent -

The Destination-System Agent is a multi-threaded code that receives file-transfer destination requests via encrypted communications from the EFTU Control Server including credentials for logon to source-system FTP service.

Receives incoming file name, source IP, hash calculation and other API parameters via AMDAS communications from the EFTU Control Server.
The FTP Client Logs onto the source-system FTP service using EFTU credentials and downloads authorized file(s) per instructions. Calculates hash and validates file integrity against source hash after the file transfer is complete.
Communicates the file status back to the EFTU Control Server.

Status-Request API -

The Status-Request API is a multi-threaded API Code to receive file transfer status requests via application calls, scripts or operator command-line execution.
It communicates with the EFTU Control Server via an AMDAS connection to get. status information. It returns status information back to the requestor

1. Describe the information (data elements) available in the system in the following categories. (Provide copy of data dictionary if available.) A. Taxpayer B. Employee (including employee log-in info) C. Other (Describe)	**A,B,&C** – Taxpayer and related tax administration data will pass through the Enterprise File Transfer Utility (EFTU). The system is not designed to be a data repository. The data receipt/send process will be point-to-point. In response to API call or script, Send transfer request from Initiating server to EFTU Control Server (a.k.a. send work order) and wait for return code – this could connect, send, receive reply, disconnect. The API Calling sequence for data will be authenticated by the 12038 database, and then transmitted to the appropriate destination named in the 12038 database. Employee log-in for this system will be restricted to System Administrator for maintenance and/or system problem resolution.
2. Describe/Identify which data elements are obtained from files, databases, individuals, or any other sources: A. IRS B. Taxpayer C. Employee D. Other Federal Agencies (List agency) E. State and Local Agencies (List agency) F. Other third party sources (Describe)	**A,B,C,D,E,F** – Only data file indicators will be passed through the EFTU 12038 database. The database will contain – File Name, File Size, File Frequency, File Owner, File Destination, Internet Protocol (IP) address for Internal customers and Password, Time of day file is processed, cycle time, file owner email and phone number, and Point of Contact for error resolution. Disclosure files are handled (transparently) just like other files, but the delivery rules specify that the second (data) file cannot be sent until the first (disclosure) file has been successfully transferred via "chained point-to-point" to its final destination (SAAS).
3. Explain why each data item is needed for the business purpose of the system.	Each data item is required to track file owner, time of file processing and security of the file.

4. a. How will each data item be verified for accuracy, timeliness and completeness?	Only the file related data elements that are required for data transfers that reside on the 12038 database are verified for authorization and authentication purposes.
4. b. Is there another source for the data that is more reliable? Explain why that source is not being used.	NO.
5. How will the data generally be retrieved by the users?	The Destination-System Agent is a multi-threaded code that receives file-transfer destination requests via encrypted communications from the EFTU Control Server including credentials for logon to source-system FTP service.
6. Can the data be retrieved by a personal identifier (name, SSN, or other unique identifier)? If yes, explain when it will be retrieved this way.	NO.

Access to the Data

7. Who will have access to the data in the system? (Users, Managers, System Administrators, Developers, Other)	Database Administrators will have access. For updating data in the 12038 database. System Administrator for routine maintenance and error resolution.
8. How is user access to the data determined and by whom? Describe the procedures and persons responsible for determining access. Include a description of the process used to determine "need to know" for different categories of users.	EFTU agents will reside on all Internal IRS platforms (CPE and Modernization). EFTU agents will communicate with the EFTU control servers using secure AMDAS (MQ-Series) messaging. AMDAS messages provide for authentication, authorization, status and control. EFTU agents initiate transfers via standard FTP services, set up by agents according to the transfer rules established when a file transfer is approved by management and security (Form 12038 plus rules definition).

9. Do other IRS systems provide, receive or share data in the system? If Yes- list the system(s) and describe which data is shared. If No, Skip to question 12.	Any authorized user in the 12038 database from any platform can transfer data with this system. The only method of access to the EFTU is through EFTU agents using secure AMDAS (MQ-Series) messaging.
10. Have the IRS systems described in Item 9 received an approved security certification and approved Privacy Impact Assessment? If yes, provide copies of memoranda.	No. The Certification and Accreditation is under way (OPR-3-0005-A00).
11. Will other agencies receive data in any form from this system? If yes, provide copy of inter-agency agreement.	No. EFTU is strictly an internal IRS system.

Administrative Controls of Data

12. What are the procedures for eliminating the data at the end of the retention period? Cite IRM reference.	The EFTU does not retain data files. EFTU is strictly a pass-through 'pilot and pull' system. No IRM is in effect for this process.
13. **A.** Does this system have new technology?	Yes. EFTU agents will communicate with the EFTU control servers using secure AMDAS (MQ-Series) messaging. AMDAS messages provide for authentication, authorization, status and control. EFTU agents initiate transfers via standard FTP services, set up by agents according to the transfer rules established when a file transfer is approved by management and security (Form 12038 plus rules definition). Transfers can be initiated by application program calls using the EFTU API, or by script or command line invocation of the agent API. All file transfers must be pre-approved and have entries in the12038 authorization database on the EFTU Control Servers.

13. **B.** How does this new technology affect taxpayer or individual privacy?	No impact on taxpayer or individual privacy.
14. Will this system have the capability to identify or locate individuals or groups? If so, describe the business purpose for this capability.	NO.
15. Will this system have the capability to monitor individuals or groups? If so, what controls are in place to prevent unauthorized monitoring?	NO.
16. Can use of the system allow IRS to treat taxpayers, employees or others differently? Explain.	NO.
17. Can the use of the system allow IRS to make determinations about individuals that would not have been possible otherwise? Explain.	NO.
18. Does the system ensure due process by allowing affected parties to respond to any determination that may harm them prior to final action? If yes, explain. If no, explain.	NO. The EFTU does not retain data files. EFTU is strictly a pass-through 'pilot and pull' system.
19. If the system is web-based, does it use persistent cookies or other tracking devices to identify the web visitor?	NO. Web interface is used for retrieving Form 12038 electronically. AMDAS communication to Source/Destination for error data transfers.